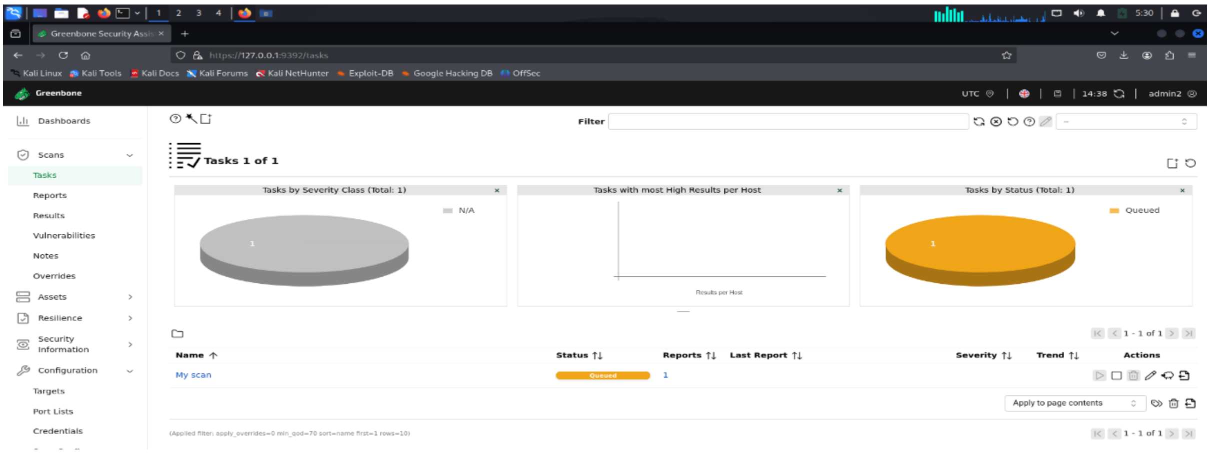
## Task 3: Vulnerability Scan Report & Analysis

### Overview

This task involved performing a **basic vulnerability scan** on my personal computer using **OpenVAS Community Edition**, a free vulnerability scanner. The goal was to identify security weaknesses, assess their severity, and research potential mitigations.

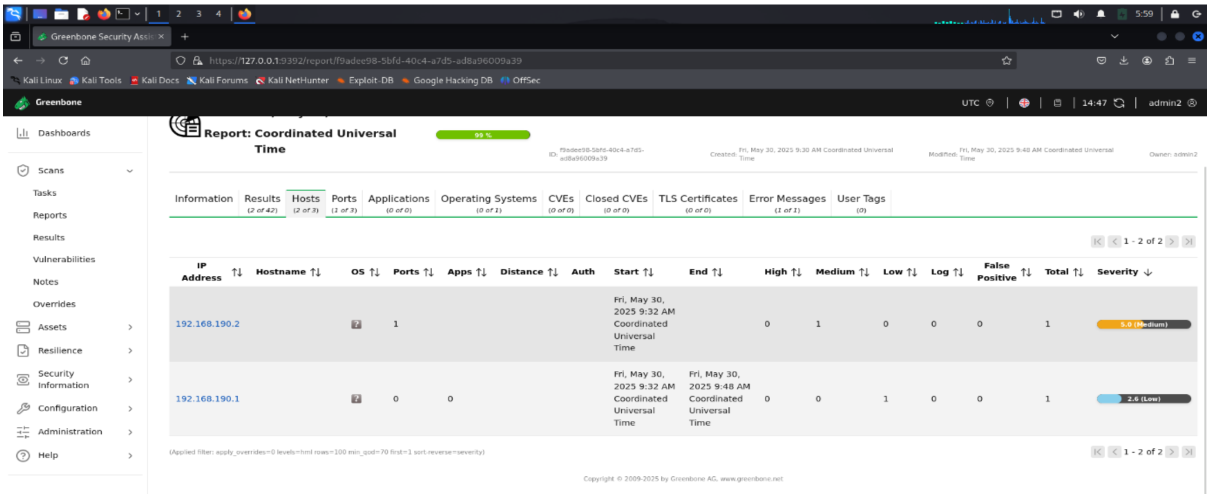
### RESULT SS



Tasks 1 of 1

| Name | Status | Reports | Last Report | Severity | Trend | Actions |
|---|---|---|---|---|---|---|
| My scan | Queued | 1 | | | | |

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)



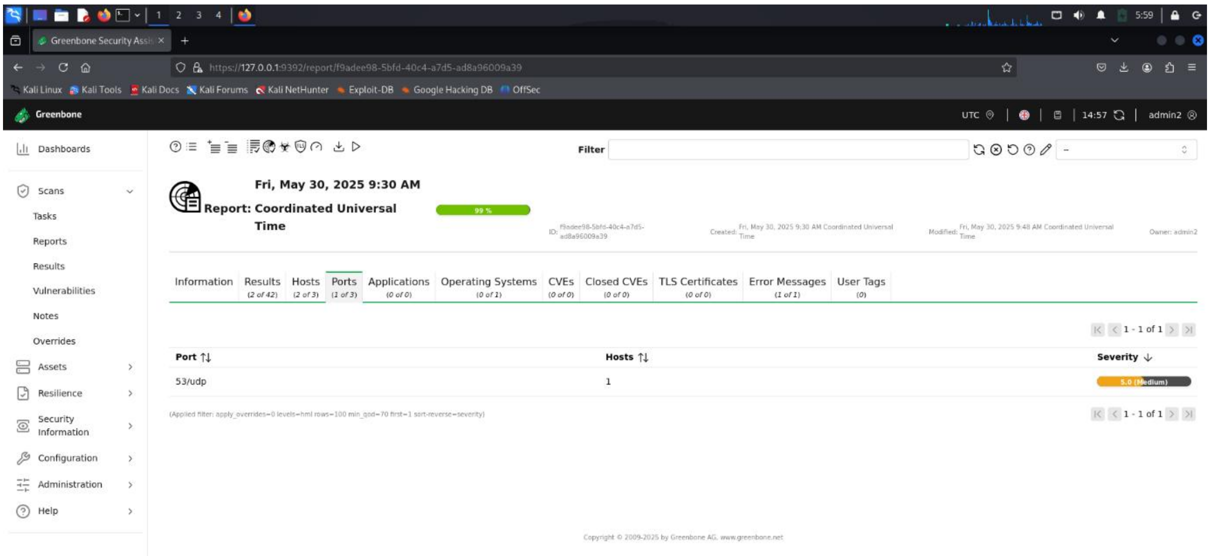
Report: Coordinated Universal Time

ID: f9adee98-5bfd-40c4-a7d5-ad8a96009a39 Created: Fri, May 30, 2025 9:30 AM Coordinated Universal Time Modified: Fri, May 30, 2025 9:48 AM Coordinated Universal Time Owner: admin2

Information | Results (2 of 42) | Hosts (2 of 3) | Ports (1 of 3) | Applications (0 of 0) | Operating Systems (0 of 1) | CVEs (0 of 0) | Closed CVEs (0 of 0) | TLS Certificates (0 of 0) | Error Messages (1 of 1) | User Tags (0)

| IP Address | Hostname | OS | Ports | Apps | Distance | Auth | Start | End | High | Medium | Low | Log | False Positive | Total | Severity |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 192.168.190.2 | | ? | 1 | | | | Fri, May 30, 2025 9:32 AM Coordinated Universal Time | | 0 | 1 | 0 | 0 | 0 | 1 | 5.0 (Medium) |
| 192.168.190.1 | | ? | 0 | 0 | | | Fri, May 30, 2025 9:32 AM Coordinated Universal Time | Fri, May 30, 2025 9:48 AM Coordinated Universal Time | 0 | 0 | 1 | 0 | 0 | 1 | 2.6 (Low) |

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)



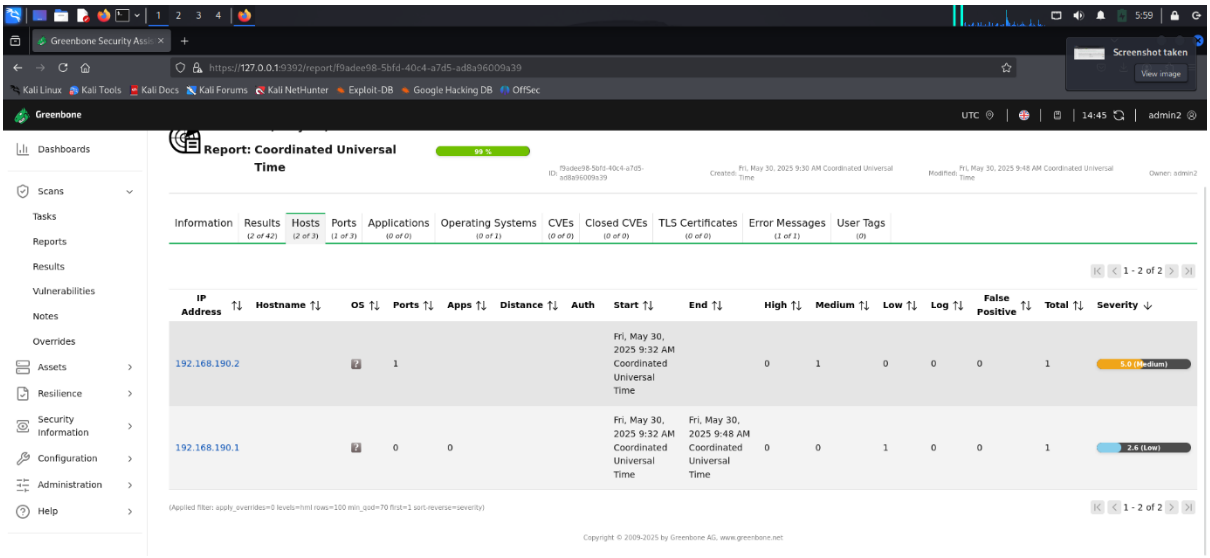
Fri, May 30, 2025 9:30 AM
Report: Coordinated Universal Time

ID: f9adee98-5bfd-40c4-a7d5-ad8a96009a39 Created: Fri, May 30, 2025 9:30 AM Coordinated Universal Time Modified: Fri, May 30, 2025 9:48 AM Coordinated Universal Time Owner: admin2

Information | Results (2 of 42) | Hosts (2 of 3) | Ports (1 of 3) | Applications (0 of 0) | Operating Systems (0 of 1) | CVEs (0 of 0) | Closed CVEs (0 of 0) | TLS Certificates (0 of 0) | Error Messages (1 of 1) | User Tags (0)

| Port | Hosts | Severity |
|---|---|---|
| 53/udp | 1 | 5.0 (Medium) |

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)



**Report: Coordinated Universal Time** 99 %

ID: f9adee98-5bfd-40c4-a7d5-ad8a96009a39 Created: Fri, May 30, 2025 9:30 AM Coordinated Universal Time Modified: Fri, May 30, 2025 9:48 AM Coordinated Universal Time Owner: admin2

Information | Results (2 of 42) | Hosts (2 of 3) | Ports (1 of 3) | Applications (0 of 0) | Operating Systems (0 of 1) | CVEs (0 of 0) | Closed CVEs (0 of 0) | TLS Certificates (0 of 0) | Error Messages (1 of 1) | User Tags (0)

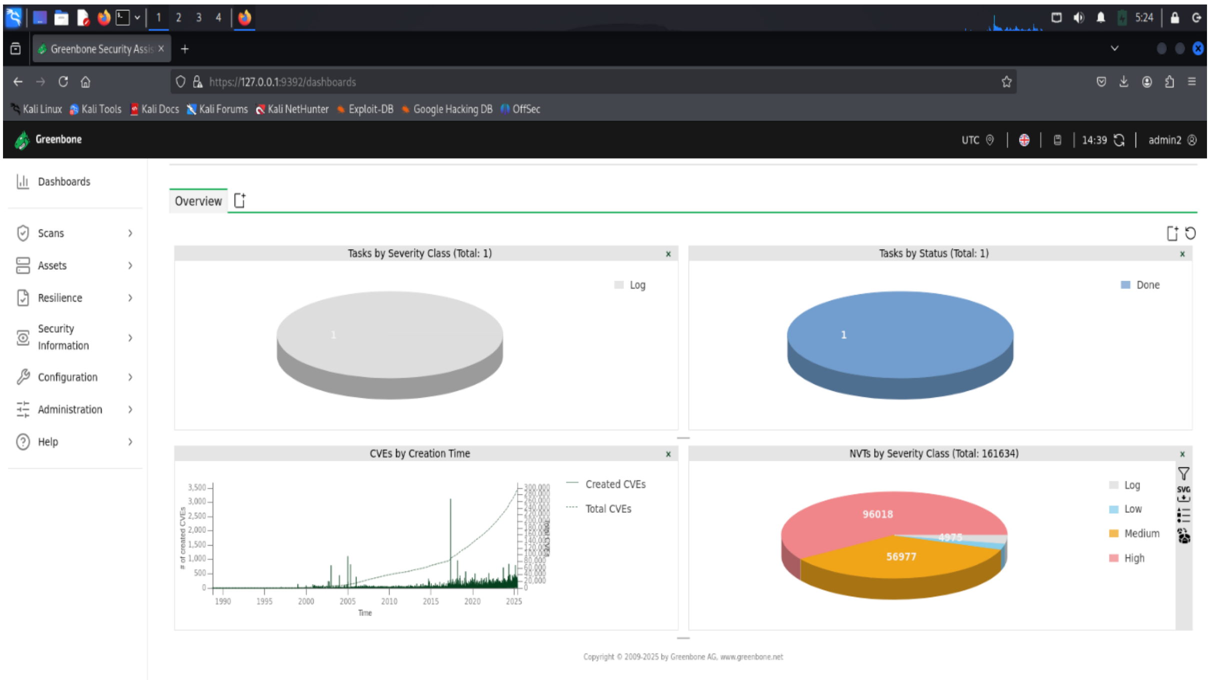
1 - 2 of 2

| IP Address | Hostname | OS | Ports | Apps | Distance | Auth | Start | End | High | Medium | Low | Log | False Positive | Total | Severity |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 192.168.190.2 | | ? | 1 | | | | Fri, May 30, 2025 9:32 AM Coordinated Universal Time | | 0 | 1 | 0 | 0 | 0 | 1 | 5.0 (Medium) |
| 192.168.190.1 | | ? | 0 | 0 | | | Fri, May 30, 2025 9:32 AM Coordinated Universal Time | Fri, May 30, 2025 9:48 AM Coordinated Universal Time | 0 | 0 | 1 | 0 | 0 | 1 | 2.6 (Low) |

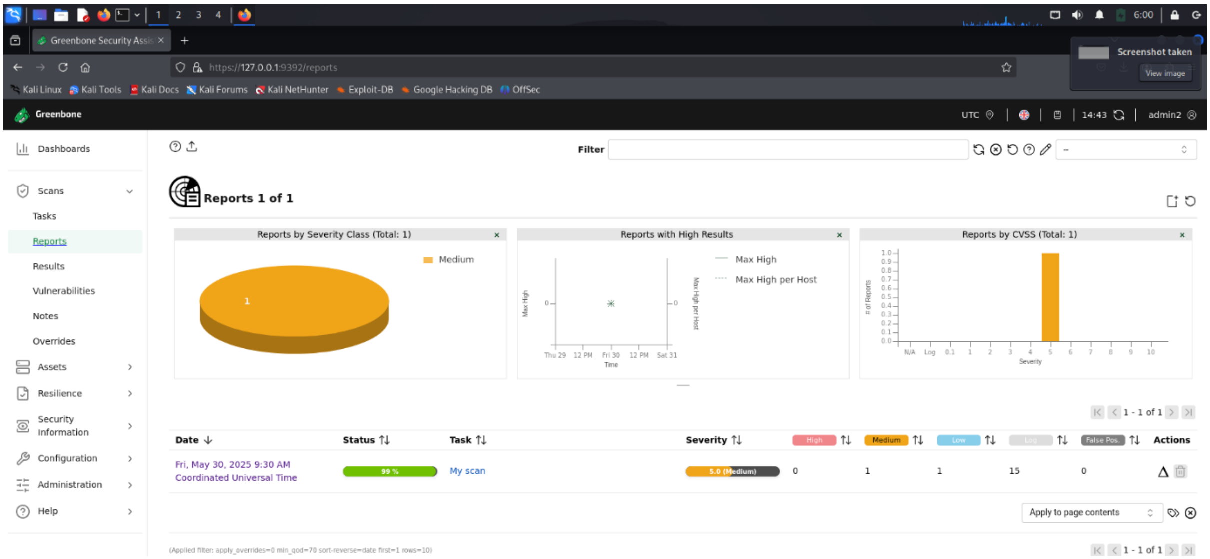
(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 2 of 2

Copyright © 2009-2025 by Greenbone AG, www.greenbone.net



Copyright © 2009-2025 by Greenbone AG, www.greenbone.net



**Reports 1 of 1**

1 - 1 of 1

| Date | Status | Task | Severity | High | Medium | Low | Log | False Pos. | Actions |
|---|---|---|---|---|---|---|---|---|---|
| Fri, May 30, 2025 9:30 AM Coordinated Universal Time | 99 % | My scan | 5.0 (Medium) | 0 | 1 | 1 | 15 | 0 | |

Apply to page contents

(Applied filter: apply_overrides=0 min_qod=70 sort-reverse=date first=1 rows=10)

1 - 1 of 1

**Target Details:**

| IP Address | Hostname | Notes |
|---|---|---|
| 192.168.190.2 | Unknown | Detected DNS cache snooping issue |
| 192.168.190.1 | Unknown | Detected TCP timestamp disclosure |

**Summary of Findings:**

| Vulnerability Title | Severity | CVSS Score | Affected IP | Port/Protocol |
|---|---|---|---|---|
| DNS Cache Snooping Vulnerability (UDP) - Active Check | Medium | 5.0 | 192.168.190.2 | 53/UDP |
| TCP Timestamps Information Disclosure | Low | 2.6 | 192.168.190.1 | TCP (general) |

**Vulnerability Details & Remediation**

**1. DNS Cache Snooping Vulnerability (UDP) – Active Check**

- **Severity**: Medium (5.0)
- **Host**: 192.168.190.2
- **Port**: 53/UDP
- **Description**: This allows an attacker to determine if a DNS server has recently resolved a specific domain name — used for reconnaissance.
- **Fix/Recommendation**:
    - Disable recursive DNS lookups for untrusted users.
    - Use firewall rules to limit DNS access to trusted hosts.
    - Monitor DNS query logs for unusual patterns.

**2. TCP Timestamps Information Disclosure**

- **Severity**: Low (2.6)
- **Host**: 192.168.190.1
- **Port**: general/tcp
- **Description**: TCP timestamps can leak system uptime, which may be used to fingerprint systems or plan exploits.
- **Fix/Recommendation**:

  - Disable TCP timestamps via OS-level configuration:
    - On Linux, add net.ipv4.tcp_timestamps = 0 to /etc/sysctl.conf
    - Apply changes using sysctl -p
  - Reboot system if required.

**Key Concepts Learned:**

- **Vulnerability scanning** helps detect weaknesses before attackers do.
- Tools like **OpenVAS** scan for known issues using signature databases.
- **CVSS (Common Vulnerability Scoring System)** is used to quantify risk.
- Even low-severity issues like information disclosure can contribute to attack chains.